

## ТЕХНІЧНІ НАУКИ

УДК 004.942

**М. М. ЗАЦЕРКЛЯНИЙ,***доктор технічних наук,**професор кафедри інформаційних систем і технологій у діяльності ОВС**Харківський національний університет внутрішніх справ***Г. С. КИРИЧЕНКО,***викладач кафедри інформаційних систем і технологій у діяльності ОВС**Харківський національний університет внутрішніх справ*

### ДОСЛІДЖЕННЯ СТЕГАНОАНАЛІТИЧНОГО МЕТОДУ ВИБІРКИ ПАР ЗА УМОВ МІНІМАЛЬНОГО ТА МАКСИМАЛЬНОГО ВБУДОВУВАННЯ

До можливих стеганоаналітичних методів належать, зокрема, статистичні методи [1; 2]. Їх особливість полягає у тому, що для певного класу зображень на їх основі можна відшукати «сталі» критерії, за допомогою яких із певною ймовірністю можна робити висновок про наявність прихованих вкладень [3].

Одним із статистичних методів стеганоаналізу є аналіз вибірки пар, розроблений Кс. Ву [4] і П. Лу [5] для аналізу фотографічних зображень. Метою даної роботи є подальше вдосконалення цього методу.

В описуваному методі зображення розбивається на пари суміжних пікселів. Позначимо ці пари  $(u, v) \in P$ , де  $P$  – множина всіх пар пікселів у зображенні. Розмір множини пар пікселів дорівнює  $P = n/2$ , де  $n$  – число пікселів. Множина  $P$  ділиться

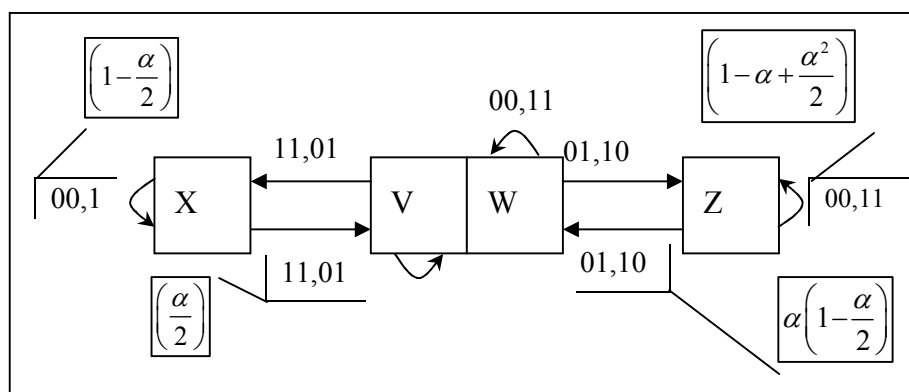
на три непересічні підмножини  $P = X \cup Y \cup Z$ . Розподіл пар на підмножини відбувається за такими правилами:

$$\begin{aligned} (u, v) \in X &\Leftrightarrow (u < v \text{ та } v - \text{парне}) \text{ або } \\ &(u > v \text{ та } v - \text{непарне}), \\ (u, v) \in Y &\Leftrightarrow (u < v \text{ та } v - \text{непарне}) \text{ або } \\ &(u > v \text{ та } v - \text{парне}), \\ (u, v) \in Z &\Leftrightarrow u = v \end{aligned} \quad (1)$$

Множина  $Y$  в свою чергу розбивається на дві підмножини  $Y = W \cup V$ , де  $(u, v) \in Y \Leftrightarrow (u, v) = (2k, 2k + 1)$  або

$$\begin{aligned} (u, v) &= (2k + 1, 2k) \\ (u, v) \in V &\Leftrightarrow (u, v) \notin W \end{aligned} \quad (2)$$

Наведені множини мають сталі ймовірності переходів (див. рис. 1).



**Рис. 1** Діаграма переходу пар пікселів між підмножинами  $Y$  та множини  $P$  для аналізу вибірки пар

На рис. 1 величина  $\alpha$  є відносною довжиною прихованого повідомлення.

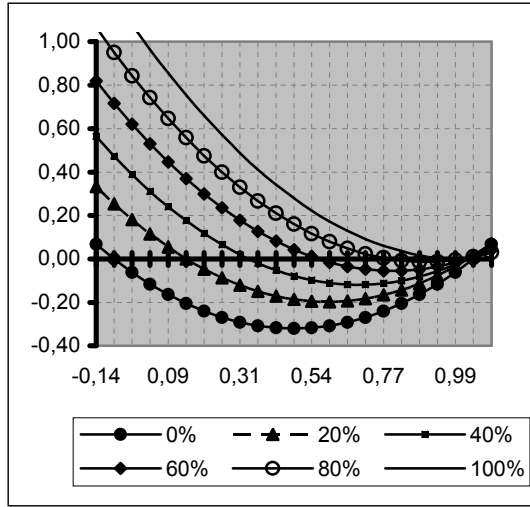
З наведеного рисунку можемо одержати залежності між множинами до та після вбудовування. Для множини  $X$ :

$$|X'| = |X| \left( 1 - \frac{\alpha}{2} \right) + |V| \frac{\alpha}{2}. \quad (3)$$

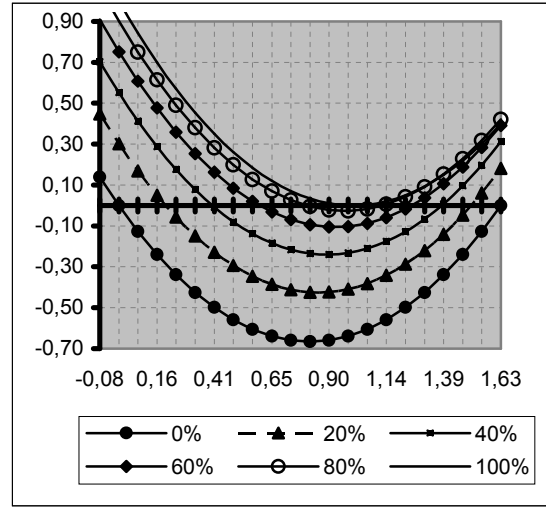
Аналогічні вирази формуються для інших множин.

У фотографічних зображеннях немає причин, аби розмір множин  $X$  та  $Y$  відрізнявся, отже:

$$|X| = |Y| \Rightarrow |X| = |V| + |W| \quad (4)$$



а)



б)

**Рис. 2. Залежність графіків функції від різних значень обсягу вбудованих даних**

Наведений підхід дозволяє досить просто визначити обсяг прихованого повідомлення, але він є непрозорим для дослідження та покращення стеганоаналітичних параметрів алгоритму. Так, із рис. 2 видно, що розташування графіків функцій, за якими відбувається визначення обсягу вбудованої інформації, відрізняє навіть для масштабованих версій того самого зображення.

Проведене дослідження доводить, що більш ефективним є визначення обсягу приховування безпосередньо з потужностей множин стегозображення. Спираючись на аналогічні припущення, що й класичний аналіз пар, та знаючи значення  $|X'|$ ,  $|V'|$ ,  $|W'|$ ,  $|Z'|$  потужностей множин після вбудовування, можна одержати системи рівнянь для визначення значень

Спираючись на це припущення та залежності, подані на рис. 1, одержуємо квадратне рівняння для знаходження  $\alpha$ :

$$\frac{1}{2}\gamma\alpha^2 + (2|X'| - |P|)\alpha + |Y'| - |X'| = 0, \quad (5)$$

де  $\gamma = |W| + |Z| = |W'| + |Z'|$ , а  $P$  – множина всіх пар пікселів у зображенні.

На рис. 2 наведені графіки функції (5) при різних значеннях обсягу ( $\alpha$ ) вбудованих даних у тестове зображення «Lena» (а) та в його збільшену версію, одержану цифровим масштабуванням (б).

$|X_0|$ ,  $|V_0|$ , а також  $|W_0|$ ,  $|Z_0|$ :

$$\begin{cases} |V_0| = \frac{|X_\alpha| + |V_\alpha| \left( \frac{\alpha}{2} - 1 \right)}{(\alpha - 1)}, \\ |X_0| = \frac{2}{\alpha} \left( |V_\alpha| - |V_0| \left( 1 - \frac{\alpha}{2} \right) \right). \end{cases}$$

$$\text{та} \begin{cases} |W_0| = \frac{(|W_\alpha| + |Z_\alpha|) \left( 1 - \alpha + \frac{\alpha^2}{2} \right) - |Z_\alpha|}{(1 - \alpha)^2}, \\ |Z_0| = \frac{|Z_\alpha| - |W_0| \left( \alpha - \frac{\alpha^2}{2} \right)}{\left( 1 - \alpha + \frac{\alpha^2}{2} \right)}, \end{cases} \quad (6)$$

де  $|X_0|$ ,  $|V_0|$ ,  $|W_0|$ ,  $|Z_0|$  – значення потужностей множин  $X$ ,  $V$ ,  $W$ ,  $Z$  до вбудовування;

$|X_\alpha|$ ,  $|V_\alpha|$ ,  $|W_\alpha|$ ,  $|Z_\alpha|$  – значення потужностей множини  $X$ ,  $V$ ,  $W$ ,  $Z$  після вбудовування псевдовипадкової послідовності

довжиною  $\alpha$ ,  $0 \leq \alpha \leq 1$ .

На рисунку 3 наведено приклад розподілу досліджуваних множин для тестового зображення «Lena» (а) та в його збільшену версію, одержану цифровим масштабуванням (б).

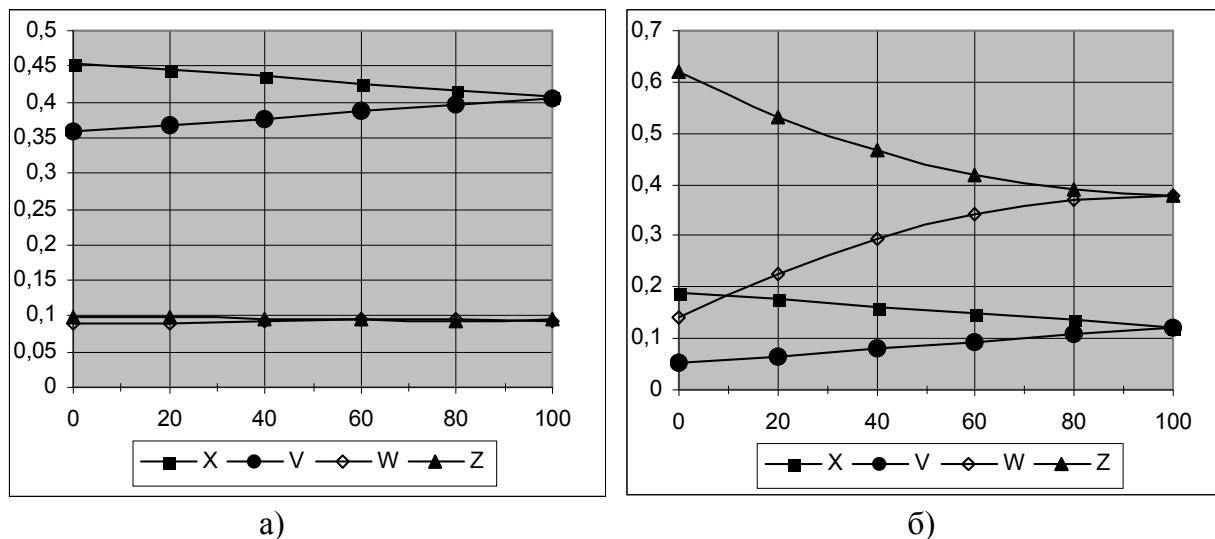


Рис. 3 Залежність потужностей множин від обсягу вбудовування

Вирази для передбачення  $X_0$ ,  $V_0$ ,  $W_0$  та  $Z_0$  показують, що при збільшенні обсягу вбудовування очікувані потужності для зображення без вбудовування  $|X_0|$  та  $|Z_0|$  збільшуються, а  $|V_0|$  та  $|W_0|$  – зменшуються. За умови справедливості виразу (4) маємо рівність  $|X_0| = |V_0| + |W_0|$ , що дозволяє з певною точністю визначити невідомий рівень вбудовування.

Розглянемо докладніше випадки вбудовувань, наближені до 0 % та 100 %.

На рисунках 4 та 5 наведено залежність функцій прогнозуючих значень  $|V_0|$  та  $|W_0|$  для граничних випадків вбудовування. Асимптотами графіків цих функцій є лінія  $x = 1$ . При максимальному вбудовуванні спостерігається наближення графіків прогнозу до асимптоти. Проведені дослідження показують досить високу точність роботи наведеного методу при граничних обсягах вбудовування.

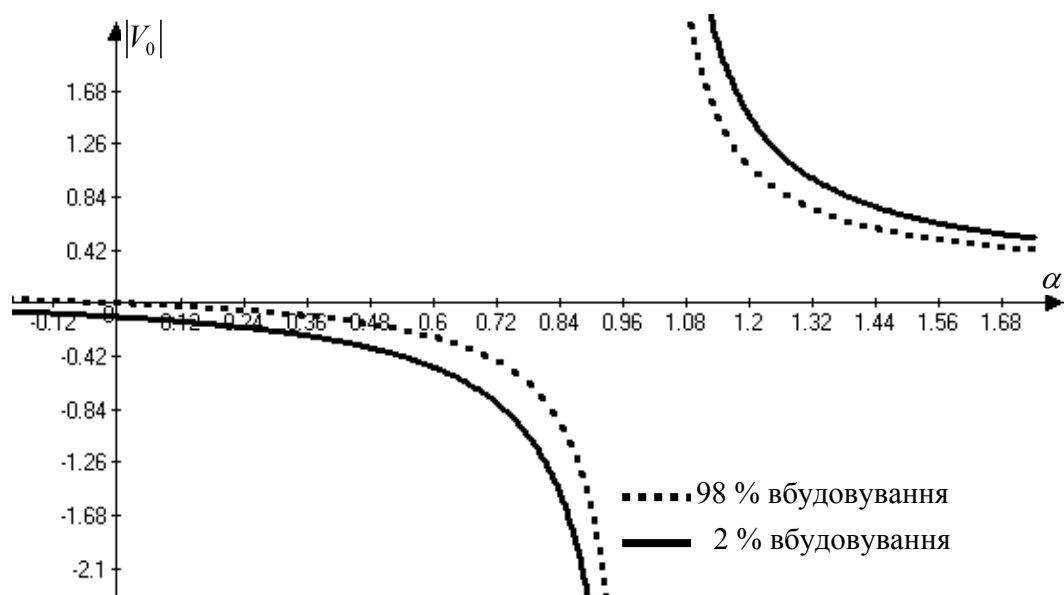


Рис. 4 Залежність  $|V_0|$  від прогнозованого значення  $\alpha$



Рис. 5 Залежність  $|W_0|$  від прогнозованого значення  $\alpha$

### Література

1. Anderson R. On the limits of steganography / R. Anderson, F. Petitcola. – IEEE J Selected Areas Commun, 1998. – P. 474–481.
2. Westfeld A. Detecting low embedding rates / Westfeld A. – Proc. Information Hiding Workshop, Springer LNCS 2578, 2002. – P. 324–339.
3. Гмурман В. Е. Теория вероятностей и математическая статистика : учеб. пособ. для вузов / Гмурман В. Е. – М. : Высш. шк., 2003. – 479 с.
4. Dumitrescu S. Detection of LSB steganography via sample pair analysis / S. Dumitrescu, X. Wu, and Z. Wang // IEEE Transactions on Signal Processing. – Pp. 1995–2007.
5. An improved sample pairs method for detection of LSB embedding / P. Lu, X. Luo, Q. Tang, L. Shen // Information Hiding [in J. Fridrich, editor]. – Berlin : 6th International Workshop, 2004. – Vol. 3200 of LNCS. – P. 116–127.

Найшла до редколегії 27.04.2009

### **Анотації**

У статті наводиться дослідження одного із статистичних методів стеганоаналізу – методу вибірки пар. Подано аналіз його працездатності на зображеннях різних типів. Вказано на недоліки методу для дослідницької діяльності у сфері стеганоаналізу. Наводяться результати досліджень працездатності нових підходів при мінімальному й максимальному обсягах вбудовування.

В статье приводится исследование одного из статистических методов стеганоанализа – метода выборки пар. Приведен анализ его работоспособности на изображениях различных типов. Указано на недостатки метода для исследовательской деятельности в сфере стеганоанализа. Приводятся результаты исследований работоспособности новых подходов при минимальном и максимальном объемах встраивания.

In the article research of one statistical method is given which is called method of pair selection. The analysis of it's capacity is resulted on the images of different types. It is indicated on inconveniences of method for steganalysis research. Results of researches with new approach are given.